UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,887	06/25/2003	Steven E. Campisi	DFC 03-1-2	4904

23531 7590 08/20/2007
SUITER SWANTZ PC LLO
14301 FNB PARKWAY
SUITE 220
OMAHA, NE 68154

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
08/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/603,887	**Applicant(s)** CAMPISI ET AL.	
	Examiner Carlton V. Johnson	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) *15 and 31-41* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14,16-30 and 42-55* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **6-7-2007**.

2. Claims **1 - 55** are pending. Claims **48 - 55** are new. Claims **1, 42, 55** have been amended. Claims **15, 31 - 41** have been cancelled. Claims **1, 42, 55** are independent.

Response to Remarks

3. Applicant's arguments filed 6/7/2007 have been fully considered but they are not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, stand-alone authentication card. (see Remarks Page 11)

The Doyle prior art discloses a smart card (authentication card) that has a processor, memory, information storage capability, which contains security related information (biometric information), encryption keys, and an attached (integrated) biometric sensor. The stored secret information (enrolled biometric information) is stored on the smart card. (see Doyle Figure 5; paragraph [0035], lines 1-7; paragraph [0036], lines 1-15: card includes means for authentication (comparison of biometric information), performed on smart card; paragraph [0035], lines 1-7: storage of biometric enrollment information) The authentication of a user is based on biometric security information on the smart card and is accomplished solely by the smart card.

3.2 Applicant argues that the referenced prior art does not disclose, an enrollment or registration procedure. (see Remarks Page 11)

The O'Gorman prior art discloses the capability for the enrollment of biometric information within the authentication system, namely the stand-alone authentication card. (see O'Gorman col. 1, lines 39-43; col. 2, lines 34-44; col. 5, lines 46-48: biometric information enrollment)

3.3 The Examiner has considered the applicant's remarks concerning a transaction authentication card that uses a biometric input and a wireless output, and power to the transaction authentication card may be accomplished through an internal battery. Biometric data used for user verification is stored on the card only and will not be transferred from the card. If authorized biometric data is authenticated, the card will transmit a wireless access code to a proximity reader or other type of transaction equipment. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Bashan (6,202,927), Doyle (20020095587), Elteto (7,111,324), Jachimowicz (5,734,154), O'Gorman (6,970,584), and Mosher (20030173408) discloses the applicant's invention including disclosures in Remarks dated June 7, 2007.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims **50, 51, 52** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. A claim in dependent form shall contain a reference to a claim previously set forth and then specify a further limitation of the subject matter claimed. Claims **50, 51, 52** refer to independent claim **31**, which has been cancelled. Claims **50, 51, 52** will be interpreted as being dependent on independent claim 1.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims **1 - 4, 7 - 10, 16 - 19, 21, 26 - 30, 48, 50, 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bashan et al.** (US Patent No. **6,202,927**) in view of **Doyle et al.** (US PGPUB No. **20020095587**) and further in view of O'Gorman (US Patent No. **6,970,584**).

Regarding Claim 1, Bashan discloses a transaction authentication card, comprising:

b) a memory; (see Bashan Figure 1; col. 2, lines 45-46: memory)

Bashan discloses wherein a processor is utilized for retrieving stored data from the memory (see Bashan col. 2, lines 51-54: processor), and a wireless transmitter capable of generating wireless signals of two different frequencies, wherein a wireless signal is transmitted (see Bashan col. 9, lines 66-67: wireless communications). Bashan does not specifically disclose a biometric identification information system.

However, Doyle discloses wherein:

a) a biometric sensor for sensing a biometric feature of a user; (see Doyle paragraph [0020], lines 1-3; paragraph [0022], lines 1-3: biometric user identification information)

c) retrieving stored biometric data representing said biometric feature from the memory, having a fingerprint matching algorithm for comparing a biometric feature of a user with the stored biometric data; (see Doyle paragraph [0026], lines 3-6: comparison of biometric information; paragraph [0035], lines 4-7: fingerprint biometric identification feature; representing said biometric feature, a fingerprint)

d) a wireless signal is transmitted on a one to one validation of the biometric feature. (see Doyle paragraph [0026], lines 3-6: comparison, (i.e. authentication, validation) of biometric identification information)

Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose self authentication and self verification. However, Doyle discloses wherein the transaction authentication card is a stand alone device and performs self authentication and self verification. (see Doyle paragraph [0035], lines 1-7; paragraph [0036], lines 1-15: card includes means for stand alone authentication and verification (comparison of biometric information), performed on smart card; paragraph [0035], lines 1-7: storage of biometric enrollment information)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability for a biometric sensor for sensing a biometric feature of a user, retrieving stored biometric data from the memory, and a processor having a fingerprint matching algorithm for comparing a biometric feature of a user with the stored biometric data, authentication. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31: " *... integrating the biometric sensor with the smart card avoids the need to transmit user authentication credentials such as a PIN over an insecure link from an input device.. ...* ")

Bashan-Doyle does not specifically disclose wherein self-enrollment. However, O'Gorman discloses wherein self-enrollment. (see O'Gorman col. 1, lines 39-43; col. 2, lines 34-44; col. 5, lines 46-48: biometric information enrollment)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability whereby the enrollment of biometric security information. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27: " ... *enclosures and data collection for sensor devices, and more particularly to a protective enclosure, which also aligns an object placed on a biometric sensor. ... "; col. 2, lines 4-7: " ... users instinctively place their fingertip on the sensor. When a fingerprint is positioned on the sensor that does not overlap the enrolled image, access will be denied due to finger placement error. ..."*)

Regarding Claim 2, Bashan discloses the transaction authentication card of Claim 1, further comprising a loop antenna, wherein the wireless transmitter is a radio frequency transmitter. (see Bashan col. 6, lines 22-26: loop antenna)

Regarding Claim 3, Bashan discloses the transaction authentication card of Claim 2, wherein a frequency of the radio frequency transmitter is between 1 KHz and 999 GHz. (see Bashan col. 9, lines 66-67: radio transmission frequency (i.e. 13.56 MHz))

Regarding Claim 4, Bashan discloses the transaction authentication card of Claim 3, wherein a wireless transmitter. (see Bashan col. 9, lines 66-67: wireless transmission) Bashan does not specifically disclose an infrared transmitter. However, Doyle discloses wherein the wireless transmitter is an infrared transmitter. (see Doyle paragraph [0011], lines 1-4: infrared wireless transmitter)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby the wireless transmitter is an infrared transmitter. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 7, Bashan discloses the transaction authentication card of Claim 1, further comprising a power supply. (see Bashan col. 2, lines 55-56; col. 4, lines 29-33: battery, power supply)

Regarding Claim 8, Bashan discloses the transaction authentication card of Claim 7, wherein the power supply is rechargeable. (see Bashan col. 3, lines 1-3: rechargeable power supply (i.e. battery))

Regarding Claim 9, Bashan discloses the transaction authentication card of Claim 7, wherein the power supply is a battery or capacitor. (see Bashan col. 2, lines 55-56; col. 4, lines 29-33: battery, power supply)

Regarding Claim 10, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card; col. 9, lines 66-67: wireless communications) Bashan does not specifically disclose the wireless signal is encoded. However, Doyle discloses wherein the wireless signal is encoded. (see Doyle paragraph [0029], lines 5-12: wireless signal encoded (i.e. encrypted)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby the wireless signal is encoded. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 16, Bashan discloses the transaction authentication card of Claim 1, further comprising a telescopic antenna coupled to the transmitter. (see Bashan col. 6, lines 22-26: antenna capability (i.e. loop or telescopic))

Regarding Claim 17, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the usage of biometric data for identification information. However, Doyle discloses wherein the memory stores biometric data for multiple users or multiple biometric data for a single user. (see Doyle paragraph [0091], lines 6-10: biometric data for multiple users; paragraph [0091], lines 11-13: multiple sets of biometric data for a single user)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby the memory stores biometric data for multiple users or multiple sets of biometric data for a single user. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 18, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose that data sent by the wireless transmitter is encrypted. However, Doyle discloses wherein data sent by the wireless transmitter is encrypted. (see Doyle paragraph [0029], lines 5-12: encryption capability)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby encryption is utilized for the secure transmission of data. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 19, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the transaction authentication card provides more than one biometric for verification. However, Doyle discloses wherein the transaction authentication card provides more than one biometric for verification. (see Doyle paragraph [0035], lines 1-16: multiple types of biometric identification information processed)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability for identification utilizing multiple types of biometric information. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 21, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose that the card is used for access control, financial transactions, security transactions, government control, airline security, passport ID, and driver's license or authentication. However, Doyle discloses wherein the card is used for access control, financial transactions, security transactions, government control, airline security, passport ID, and driver's license or authentication. (see Doyle paragraph [0086], lines 4-7; paragraph [0086], lines 16-20: card utilized for authentication and security related transactions)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable that the card is used for access control, financial transactions, security transactions, government control, airline security, passport ID, and driver's license or authentication. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 26, Bashan discloses the transaction authentication card of Claim 1, wherein the wireless transmitter is an RF transmitter that operates between 1 KHz and 999 GHz. (see Bashan col. 9, lines 66-67: wireless communications (i.e. 13.56 MHz frequency))

Regarding Claim 27, Bashan discloses the transaction authentication card of Claim 26, further comprising an RF receiver that is capable of receiving a signal between 1 KHz and 999 GHz. (see Bashan col. 9, lines 66-67: wireless communications (i.e. 13.56 MHz frequency)).

Regarding Claim 28, Bashan discloses the transaction authentication card of Claim 1, further comprising one or more batteries that supply power to the biometric sensor, the memory, the processor, and the wireless transmitter on the card. (see Bashan Figure 1; see Bashan col. 2, lines 55-56; col. 4, lines 29-33: battery, power supply)

Regarding Claim 29, Bashan discloses the transaction authentication card of Claim 1, wherein the card has a portable database and does not require an external source for biometric enrollment or verification. (see Bashan col. 2, lines 45-46: storage (i.e. memory) within card, internal)

Regarding Claim 30, Bashan discloses the transaction authentication card of Claim 1, wherein the processor uses industry standard minutia points for verification. (see Doyle paragraph [0035], lines 4-7: fingerprint biometric identification information utilizes minutia points)

Regarding Claim 48, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose a biometric sensor cover access port. However, O'Gorman disclose wherein a biometric sensor cover access port. (see O'Gorman col. 3, lines 6-9; col. 3, lines 26-28: biometric sensor cover)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability whereby a biometric sensor cover access port. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27; col. 2, lines 4-7)

Regarding Claim 50, Bashan discloses the method of Claim 31. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the step of generating a serial number based on the biometric input. However, Doyle discloses wherein the step of generating a serial number based on the biometric input. (see Doyle paragraph [0097], lines 1-5: identifier (i.e. serial number) generated for data processing)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby the step of generating a serial number based on the biometric input. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Regarding Claim 55, Bashan discloses a transaction authentication card, comprising:

b) a memory; (see Bashan Figure 1; col. 2, lines 45-46: memory)

Bashan discloses wherein a processor retrieving data from memory. (see Bashan col. 2, lines 51-54: processor) Bashan does not specifically disclose a biometric identification information system.

However, Doyle discloses:

a) a biometric sensor for sensing a biometric feature of a user; (see Doyle paragraph [0020], lines 1-3; paragraph [0022], lines 1-3: biometric for user identification information)

c) retrieving stored biometric data from the memory, the processor having a fingerprint matching algorithm for comparing a biometric feature of a user with the stored biometric data and a serial number generation algorithm for generating a serial number based on the fingerprint matching algorithm; (see Bashan col. 2, lines 51-54: processor; (see Doyle paragraph [0026], lines 3-6: comparison of biometric information; paragraph [0035], lines 4-7: fingerprint biometric identifying feature; paragraph [0097], lines 1-5: identifier (i.e. serial number) generated for data processing))

Bashan-Doyle discloses wherein a wireless transmitter capable of generating wireless signals, wherein a wireless signal is transmitted on a one to one validation of the biometric feature. (see Bashan col. 9, lines 66-67: wireless communications; col. 2, lines 61-65: different frequencies)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby retrieving stored biometric data from the memory, the processor having a fingerprint matching algorithm for comparing a biometric feature of a user with the stored biometric data and a serial number generation algorithm for generating a serial number based on the fingerprint matching algorithm. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Bashan-Doyle discloses wherein storage of said biometric data representing said biometric feature of said user. (see Doyle paragraph [0035], lines 1-7: storage of biometric information) Bashan-Doyle does not disclose whereby said processor is configured for enrollment of said biometric feature of said user.

However, O'Gorman discloses:

d) wherein said processor is configured for enrollment of said biometric feature of said user and said biometric feature of said user acquired during enrollment within said first memory: (see O'Gorman col. 1, lines 39-43; col. 2, lines 34-44; col. 5, lines 46-48: biometric information enrollment)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability whereby the enrollment of biometric security information. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27; col. 2, lines 4-7)

8. Claims **5,** 6, **11 - 13** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bashan-Doyle-O'Gorman** and further in view of **Elteto et al.** (US Patent No. **7,111,324**).

Regarding Claim 5, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the wireless signal is formatted as a human interface device (HID) signal. However, Elteto discloses wherein the wireless signal is formatted as a human interface device (HID) signal. (see Elteto col. 4, line 64 - col. 5, line 14: data transfer between card equivalent device (i.e. token) and access device via USB interface using standard USB protocol)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Elteto to enable the capability whereby the wireless signal is formatted as a human interface device (HID) signal or USB standard signal interface. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62: " *... there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces. ...* ")

Regarding Claim 6, Bashan discloses the transaction authentication card of Claim 5, wherein the human interface device signal is compatible with Mifare. (see Bashan col. 9, lines 66-67: Mifare frequency (i.e. 13.56 MHz), wireless communications capability)

Regarding Claim 11, Bashan discloses the transaction authentication card of Claim 1, further comprising a multicolor light emitting diode. (see Bashan col. 10, lines 41-45: LED indicator utilized as alert or status indicator) Bashan does not specifically disclose a multicolor light emitting diode. However, Elteto discloses wherein a multicolor light emitting diode. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as status indication)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Elteto to enable the capability to utilize multi-color light emitting diodes for a status indication. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62: " ... From the foregoing, it can be seen that there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces. ... ")

Regarding Claim 12, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card; col. 10, lines 41-45: LED indicator utilized as alert or status indicator) Bashan does not specifically disclose the multicolor light emitting diode indicates a first color for a good read and a second color for a low battery. However, Elteto discloses wherein the multicolor light emitting diode indicates a first color for a good read and a second color for a low battery. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as a status (i.e. good read, low battery) indication)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Elteto to enable the capability for the multicolor light emitting diode to indicate a first color for a good read and a second color for a low battery. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62)

Regarding Claim 13, Bashan discloses the transaction authentication card of Claim 12. (see Bashan col. 2, lines 37-43: transaction card; col. 10, lines 41-45: LED indicator utilized as alert or status indicator) Bashan does not specifically disclose the multicolor light emitting diode indicates a third color for a state of enrollment. However, Elteto discloses wherein the multicolor light emitting diode indicates a third color for a state of enrollment. (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as a status (i.e. good read, low battery) indication)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Elteto to enable the capability whereby the multicolor light emitting diode indicates a third color for a state of enrollment. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62)

9. Claims **14, 20, 22 - 25** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bashan-Doyle-O'Gorman** and further in view of **Jachimowicz et al.** (US Patent No. **5,734,154**).

Regarding Claim 14, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the transaction authentication card is used with a financial transaction terminal or an automated teller machine terminal. However, Jachimowicz discloses wherein the transaction authentication card is used with a financial transaction terminal. (see Jachimowicz Figure 1; col. 9, lines 47-50: bank or financial transaction information accessed)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Jachimowicz to enable the capability for usage in a financial transaction. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37: *" ... provide new and improved apparatus for viewing information stored on a smart card, which apparatus contains safe features to prevent unwarranted viewing of the information. ... "*)

Regarding Claim 20, Bashan discloses the transaction authentication card of Claim 1, wherein further comprising a processor. (see Bashan col. 2, lines 51-54: processor; col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the biometric sensor is on a front side of the card. However, Doyle discloses wherein a biometric sensor is on a front side of card.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Doyle to enable the capability whereby a biometric sensor is on a front side of card. One of ordinary skill in the art would have been motivated to employ the teachings of Doyle in order to avoid the transmission of user authentication information over insecure links. (see Doyle paragraph [0080], lines 28-31)

Bashan-Doyle does not specifically disclose wherein an image is formed on a back side of the card. However, Jachimowicz discloses an image is formed on a back side of the card. (see Jachimowicz Figure 14; col. 1, lines 49-51: display for image viewing, image viewed through aperture)

It would have been obvious to one of ordinary skill in the art to modify Bashan-Doyle as taught by Jachimowicz to enable the capability whereby an image is formed on a back side of the card. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

Regarding Claim 22, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose a display for showing an image downloaded by a user. However, Jachimowicz discloses wherein further comprising a display for showing an image downloaded by a user. (see Jachimowicz col. 1, lines 49-51: display for image viewing)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Jachimowicz to enable the capability for a display for showing an image downloaded by a user. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

Regarding Claim 23, Bashan discloses the transaction authentication card of Claim 22. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose wherein the image is a photo id. However, Jachimowicz discloses wherein the image is a photo id. (see Jachimowicz col. 1, lines 49-51: display for image (i.e. photo id) viewing)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Jachimowicz the capability wherein the image is a photo id. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

Regarding Claim 24, Bashan discloses the transaction authentication card of Claim 22. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose wherein the displayed image is text. However, Jachimowicz discloses wherein the image is text. (see Jachimowicz Figure 14; col. 1, lines 49-51: display for image or text viewing)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Jachimowicz to enable the capability whereby a display image is text. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

Regarding Claim 25, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically discloses an alphanumeric keypad membrane for personal identification entry. However, Jachimowicz discloses wherein an alphanumeric keypad membrane for personal identification entry. (see Jachimowicz col. 3, lines 18-25: keypad membrane for data input)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Jachimowicz to enable a keypad type data input capability. One of ordinary skill in the art would have been motivated to employ the teachings of Jachimowicz in order to provide an improved apparatus for viewing the information stored on a smart card. (see Jachimowicz col. 1, lines 34-37)

10. Claims **42 - 47** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doyle** in view of **Elteto et al.** (US Patent No. **6,970,584**) and further in view of O'Gorman.

Regarding Claim 42, Doyle discloses a transaction authentication card, comprising:

a) a body in the general form of a rectangular solid having a substantially hollow interior, the body measuring between 1 to 5 inches on a first side, 1 to 4 inches on a second side substantially perpendicular to the first side, and 1/8 to 1/2 inch on a third side substantially perpendicular to the first and second sides, the body being formed of impact plastics. (see Doyle paragraph [0022], lines 1-3;

paragraph [0080], lines 28-31: smart card utilizing standard smart card dimensions, and plastic construction)

b) a fingerprint sensor for sensing minutia points of a fingerprint of a user, the fingerprint sensor being mounted to an inside of the body such that a sensing portion of the fingerprint sensor is exposed through an opening in the body; (see Doyle paragraph [0020], lines 1-3; paragraph [0022], lines 1-3: biometric sensor integrated with card for user identification information; paragraph [0035], lines 4-7: fingerprint specific processing)

c) a first memory and a second memory, the first memory storing a database of enrolled fingerprints and the second memory being a read only memory for storing an identification code for the transaction authentication card, the identification code serving to identify the card to an access control device; (see Doyle paragraph [0035], lines 4-7: fingerprint specific biometric identification information captured; paragraph [0025], lines 9-11; paragraph [0036], lines 1-6: fingerprint storage; paragraph [0097], lines 1-5: identifier for device (i.e. card))

d) a processor (see Doyle paragraph [0111], lines 8-16: processor) for retrieving stored biometric data representing a biometric feature of said user from the first memory, the processor having a fingerprint matching algorithm for comparing said biometric feature of a user with the stored biometric data, the processor reading a fingerprint pattern from the fingerprint sensor, the processor sending a signal to be transmitted; (see Doyle paragraph [0026], lines 3-6: comparison, (i.e. authentication, validation) of biometric (i.e. fingerprint) identification information)

e) an encrypter for encrypted the signal to be transmitted; (see Doyle paragraph [0029], lines 5-12: encryption capability for communications)

f) a radio frequency (RF) transmitter for transmitting the encrypted signal on a one to one validation of the fingerprint of the user, the RIF transmitter capable of transmitting a first RF signal of a first frequency and a second RF signal of a second frequency, wherein the first frequency is between 100 KHz and 200 KHz and the second frequency is between 10 MHz and 20 MHz; (see Doyle paragraph [0029], lines 5-7; paragraph [0047], lines 1-2; paragraph [0051], lines 4-11: wireless communications (i.e. 13.56 MHz frequency, different frequencies; paragraph [0057], lines 7-15; paragraph [0008], lines 13-19: radio, short range, proximity));

g) an antenna coupled to the RF transmitter for transmitting the RF signal; (see Doyle paragraph [0057], lines 7-15: antenna capability)

Doyle does not specifically disclose multi-color light emitting diodes as status indicators.

However, Elteto discloses:

h) a three color light emitting diode mounted on the body such that a first color indicates a first condition, a second color indicates a second condition, and a third color indicates a third condition; (see Elteto col. 14, lines 21-28; col. 14, lines 55-61: multi-color LED display as status indication)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Elteto to enable the capability whereby a first color indicates a first condition, a second color indicates a second condition, and a third color indicates a third condition. One of ordinary skill in the art would have been motivated to employ the teachings of Elteto in order to enable the retrieval of security information without requiring the usage of insecure interfaces. (see Elteto col. 3, lines 59-62: " ... From the foregoing, it can be seen that there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces. ... ")

Doyle discloses wherein an internal power supply for powering all circuitry with the card. (see Doyle paragraph [0057], lines 7-15: power supply, batteries), and storage of said biometric data representing said biometric feature of said user. (see Doyle paragraph [0035], lines 1-7: storage of biometric information) Doyle-Elteto does not specifically disclose whereby said processor is configured for enrollment of said biometric feature of said user.

However, O'Gorman discloses:

i) wherein said processor is configured for enrollment of said biometric feature of said user and storage of said biometric data representing said biometric feature of said user acquired during enrollment within said first memory. (see O'Gorman col. 1, lines 39-43; col. 2, lines 34-44; col. 5, lines 46-48: biometric information enrollment)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability whereby the enrollment of biometric security information. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27; col. 2, lines 4-7)

Regarding Claim 43, Doyle discloses the transaction authentication card of Claim 42, wherein the body measures 3 3/8 x 2 1/8 x 3/16 inches. (see Doyle paragraph [0022], lines 1-3; paragraph [0080], lines 28-31: smart card utilizing standard smart card dimensions, and plastic construction)

Regarding Claim 44, Doyle discloses the transaction authentication card of Claim 42, wherein the first frequency is 13.56 MHz and the second frequency is 125 KHz. (see Doyle paragraph [0029], lines 5-7; paragraph [0047], lines 1-2; paragraph [0051], lines 4-11: wireless communications (i.e. 13.56 MHz frequency, different frequencies, short range, proximity))

Regarding Claim 45, Doyle discloses the transaction authentication card of Claim 42, wherein the first frequency is 15.76 MHz and the second frequency is 129 KHz. (see Doyle paragraph [0029], lines 5-7; paragraph [0047], lines 1-2; paragraph [0051], lines

4-11: wireless communications (i.e. 13.56 MHz frequency, different frequencies, short range, proximity))

Regarding Claim 46, Doyle discloses the transaction authentication card of Claim 44, wherein the antenna is a loop antenna. (see Doyle paragraph [0057], lines 7-15: antenna capability)

Regarding Claim 47, Doyle discloses the transaction authentication card of Claim 44, wherein the antenna is a telescopic antenna. (see Doyle paragraph [0057], lines 7-15: antenna capability)

11. Claims **49, 51, 52** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bashan-Doyle-O'Gorman** and further in view of **Mosher, JR et al.** (US PGPUB No. **20030173408**).

Regarding Claim 49, Bashan discloses the transaction authentication card of Claim 1. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose a system for erasing data. However, Mosher discloses wherein a system for erasing data. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Mosher to enable the capability whereby a system for erasing data. One of ordinary skill in the art would have been motivated to employ the teachings of Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8: " ... *wireless communications and data storage functions, opportunities for falsification and fraudulent use are increased. Of concern are insuring tamper detection, tamper prevention, secure transmission of information, the integrity of the information, and the prevention of unauthorized transfer of the information to others. Improvements in each of these areas are needed. ...* ")

Regarding Claim 51, Bashan discloses the method of Claim 31. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose a biometric sensor cover access port. However, O'Gorman disclose wherein a biometric sensor cover access port. (see O'Gorman col. 3, lines 6-9; col. 3, lines 26-28: biometric sensor cover)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability engaging a biometric sensor cover access port. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27*; col. 2, lines 4-7*)

Bashan-Doyle-O'Gorman does not specifically disclose enabling the transaction authentication card to be cleared and used again. However, Mosher discloses wherein enabling the transaction authentication card to be cleared and used again. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Mosher to enable the capability whereby enabling the transaction authentication card to be cleared and used again. One of ordinary skill in the art would have been motivated to employ the teachings of Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8)

Regarding Claim 52, Bashan discloses the method of Claim 31. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose the step of erasing the transaction authentication card. However, Mosher discloses wherein the step of erasing the transaction authentication card. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Mosher to enable the capability whereby the step of erasing the transaction authentication card. One of ordinary skill in the art would have been motivated to employ the teachings of Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8)

12. Claims **53, 54** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doyle-Elteto-O'Gorman** and further in view of **Mosher**.

Regarding Claim 53, Bashan discloses the transaction authentication card of Claim 42. (see Bashan col. 2, lines 37-43: transaction card)

Bashan does not specifically disclose a biometric sensor cover access port. However, O'Gorman disclose wherein a biometric sensor cover access port. (see O'Gorman col. 3, lines 6-9; col. 3, lines 26-28: biometric sensor cover)

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by O'Gorman to enable the capability engaging a biometric sensor cover access port. One of ordinary skill in the art would have been motivated to employ the teachings of O'Gorman in order to enable a protective enclosure, which also aligns object placement on sensor. (see O'Gorman col. 1, lines 24-27*; col. 2, lines 4-7*)

Bashan-Doyle-O'Gorman does not specifically disclose to enable the transaction authentication card to be cleared and used again. However, Mosher discloses wherein to enable the transaction authentication card to be cleared and used again. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Mosher to enable the capability whereby to enable the transaction authentication card to be cleared and used again. One of ordinary skill in the art would have been motivated to employ the teachings of Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8)

Regarding Claim 54, Bashan discloses the transaction authentication card of Claim 42. (see Bashan col. 2, lines 37-43: transaction card) Bashan does not specifically disclose a system for erasing data if the body is opened. However, Mosher disclose wherein a system for erasing data if the body is opened. (see Mosher paragraph [0070], lines 3-10; paragraph [0071], lines 8-17; paragraph [0098], lines 31-33: erasure capability for data)

The only disclosure within the specification of an erasure of data is when power source is shutdown. There is no disclosure within specification of an erasure of data via a command sequence or any other action.

It would have been obvious to one of ordinary skill in the art to modify Bashan as taught by Mosher to enable the capability whereby a system for erasing data if the body is opened. One of ordinary skill in the art would have been motivated to employ the teachings of Mosher in order to enable tamper detection, tamper prevention, secure transmission of information, and the integrity of the information, and the capability to prevent the unauthorized transfer of the information to others. (see Mosher paragraph [0006], lines 4-8)

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
August 6, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/16/07